

Centralized Auditing in Windows

Derek Melber

Introduction

As I have been speaking, evangelizing, educating, and writing about Windows operating systems for the past 15 years, I have heard one common request during that time. "How do I centralize the logs generated in the Event Viewer from different computers?" My answer has always been to use a third party product since Microsoft solutions do not support this feature. However, with the release of Windows Server 2008 and Windows Vista, centralized logging is possible. Before you stop reading this article because you do not have a Windows Server 2008 or Vista setup, please read on! Microsoft has designed the centralized logging to report to a Windows Server 2008 or Vista computer but has also made it backward compatible for Windows Server 2003 and Windows XP clients. That is right, as long as you have one Windows Server 2008 OR Windows Vista computer, you can have centralized logging for your Windows computers.

Requirements and Configuration for Centralized Logging Computer

Any Windows Server 2008 or Windows Vista computer can become your centralized log computer. This means that all logs that you configure on your Windows Server 2008, Windows Server 2003, Windows Vista, or Windows XP computers will be sent to this centralized log computer for a one stop shop of all key events.

If you want your Windows Server 2008 computer or Vista to hold the centralized log, there is really not all that much that needs to be done. However, you do need to configure the computer to support the log; you can do this by running a few commands from an elevated command prompt.

Note: The command prompt must be elevated when User Account Control is enabled.

The first command you need to run will set up the Remote Management on the computer. It is the following command:

```
winrm qc
```

This command will generate a response informing you that certain tasks need to be performed by the system, and you just need to confirm "Yes" that you want them done. The message can be seen in Figure 1.

Note: If you use the `-q` switch at the end of your command, the command and actions will perform automatically and silently.

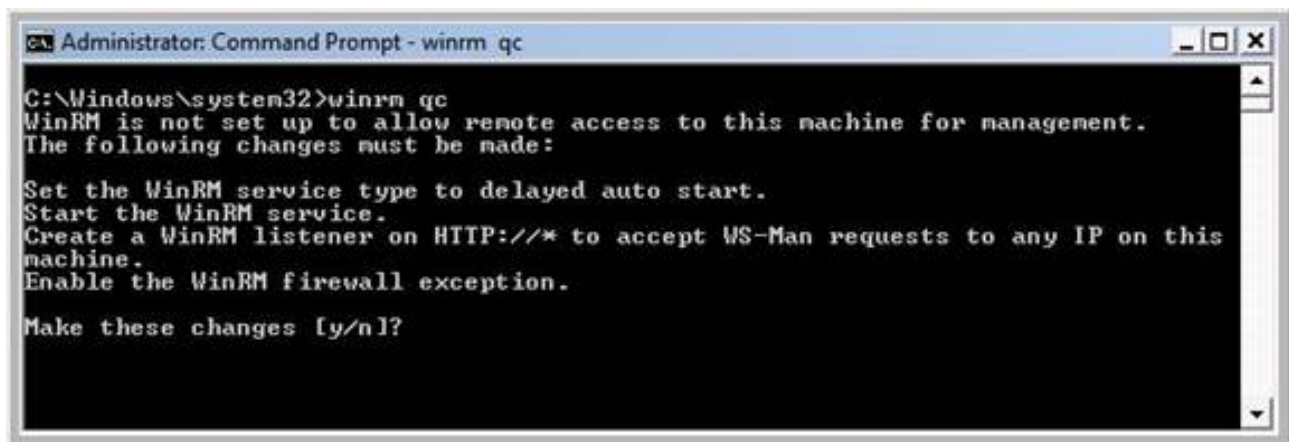


Figure 1: Configuring remote management on a Windows Vista computer

Centralized Auditing in Windows

Derek Melber

After entering Y to make the changes, results will instantly appear indicating that the actions were successful.

The second command will configure the Event Collector service. This command is similar, but controls the Event Collector service:

```
wecutil qc /q
```

Again, you will receive confirmation that the action was successful.

Requirements and Configuration for Centralized Logging Computer

If you are using Windows Server 2008 or Windows Vista as the source computer, then you only need to run a command to get the computer ready to forward to the centralized log computer. This is the same command that you used for the centralized computer to get the remote management setup correctly:

```
winrm qc -q
```

If you are using Windows Server 2003 or XP, you will need to download and install the Forwarding aspect of the remote management for the operating systems.

Note: You must have SP1 for Windows Server 2003 and SP2 for Windows XP installed before you can configure forwarding correctly.

You can download the installation bits here. After installation, you then run the same remote management configuration string:

```
winrm qc -q
```

Note: You must have administrative credentials to perform this configuration.

You can check that the configuration worked by launching the Event Viewer. When Event Viewer is up, then you should see a new node named Microsoft-Windows-Forwarding/Operational, as shown in Figure 2.

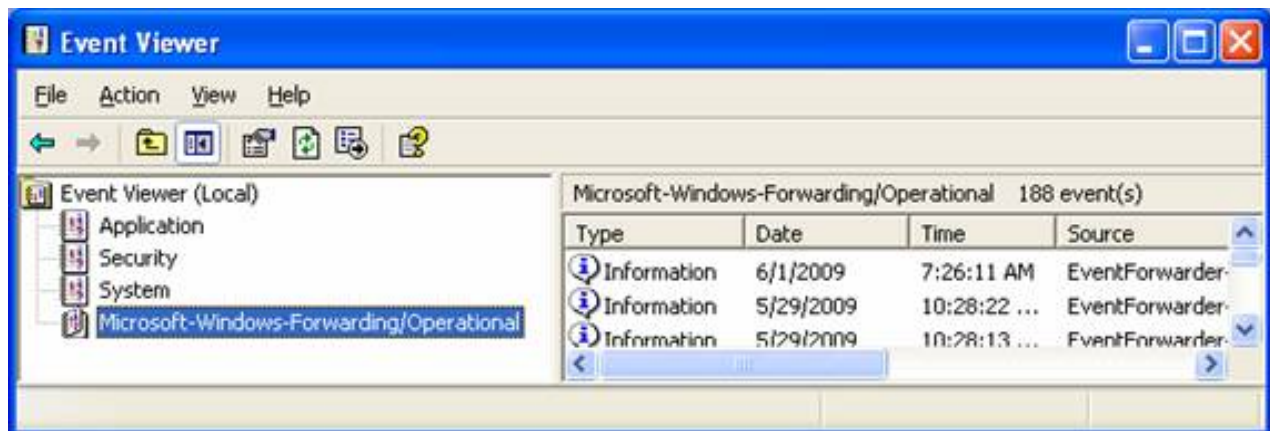


Figure 2: Windows XP forwarding log in Event Viewer

Centralized Auditing in Windows

Derek Melber

Setting up a Subscription

The configuration of subscriptions is performed on the centralized log computer. For these steps, you will need to configure the following:

- Computer name that you want to collect information from
- Event type (critical, error, warning, etc.)
- By log (System, application, etc)
- By source (Huge list of options!)
- Event ID(s) (typically won't want to collect all of them, so list them with commas between the numbers)
- Keywords
- User or Computer

Note: Not all of these are required, but they are available options!

Your first step is to determine which computer you want to collect information from. This is done by right-clicking on the Subscriptions node in Event Viewer, then selecting Create Subscription. In the Subscription Properties box, select the Select Computers button, as seen in Figure 3.

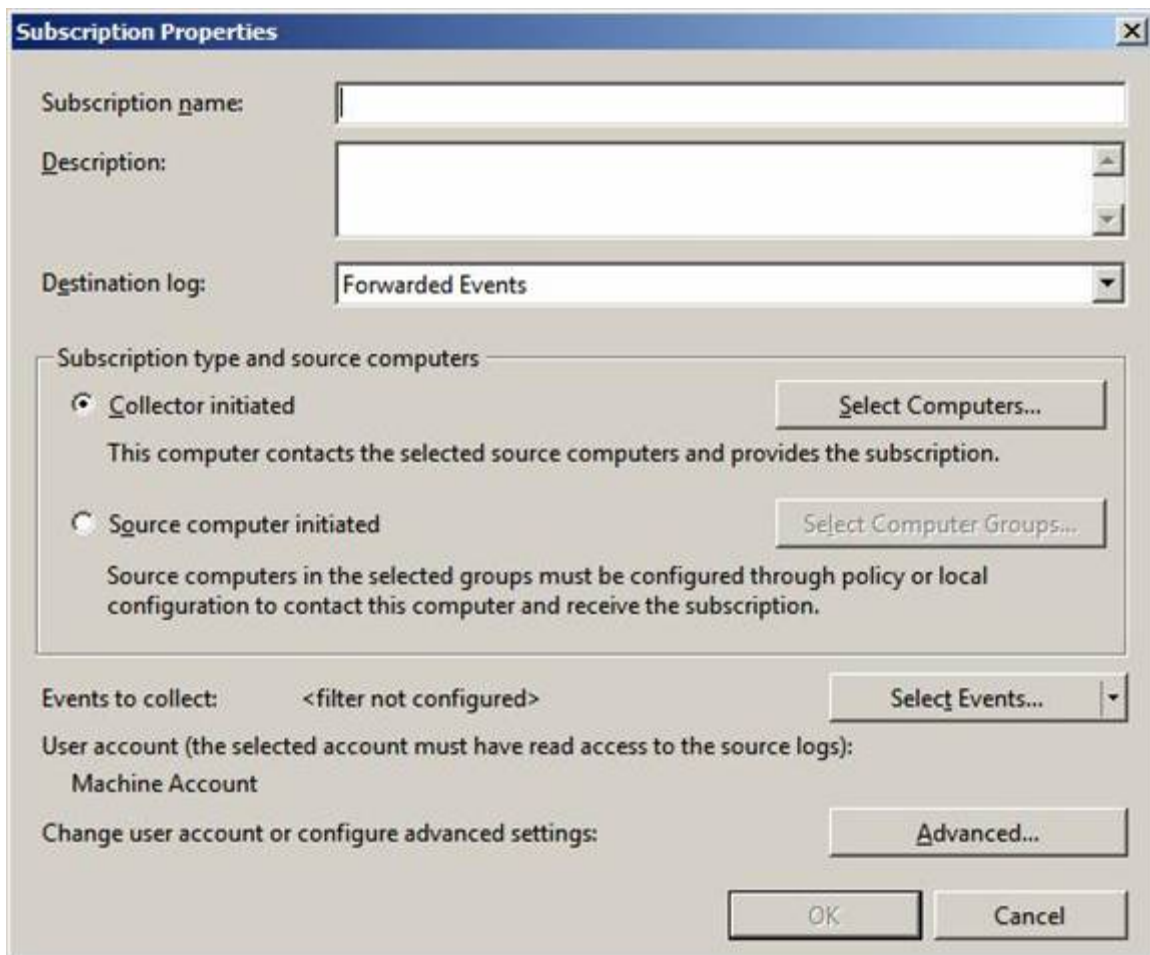


Figure 3: Subscription Properties dialog box allows you to configure your logs to collect

Centralized Auditing in Windows

Derek Melber

Within the computer selection dialog box, you can Add Domain Computers to the list of computers you want to collect log entries from. This is helpful, as you can create one subscription to collect similar events from many computers with only one set of events defined. You also have a Test option, to ensure that the centralized computer can see the remote computer from which it is collecting events, which is shown in Figure 4.

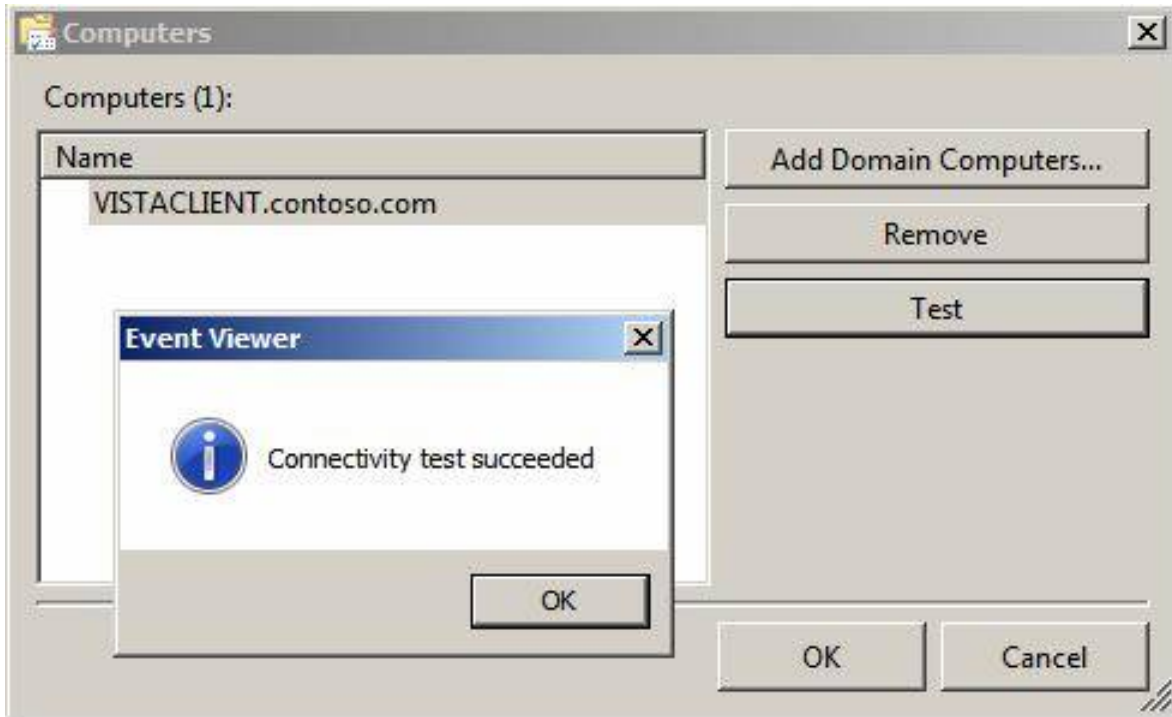


Figure 4: You can test to ensure the computer you are collecting from is configured correctly

After configuring the computers you want to collect from, now you only need to configure the events and details of what you want to collect. Figure 5 illustrates what your options are.

Centralized Auditing in Windows

Derek Melber

Query Filter

Filter XML

Logged: Any time

Event level: Critical Warning Verbose
 Error Information

By log By source

Event logs:

Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel

Figure 5: Each subscription allows you to be very detailed on what you want to collect

After you configure which events you want to collect, based on the myriad of options you have available, you just need to wait for the events to be collected on the source computer and sent to the centralized log computer.

Viewing Collected Events

To view the collected events on your centralized log computer, you just need to go to Event Viewer. There, you will see a node under the Windows Logs named Forwarded Events. The source computer is configured to send all events to this location. You can of course set up Custom Views to separate and organize your events into other custom logs (which might be beneficial if you are collecting from many computers and collecting different types of events). Figure 6 illustrates a sample set of events that are being collected from a Windows XP computer to a Windows Server 2008 computer.

Centralized Auditing in Windows

Derek Melber

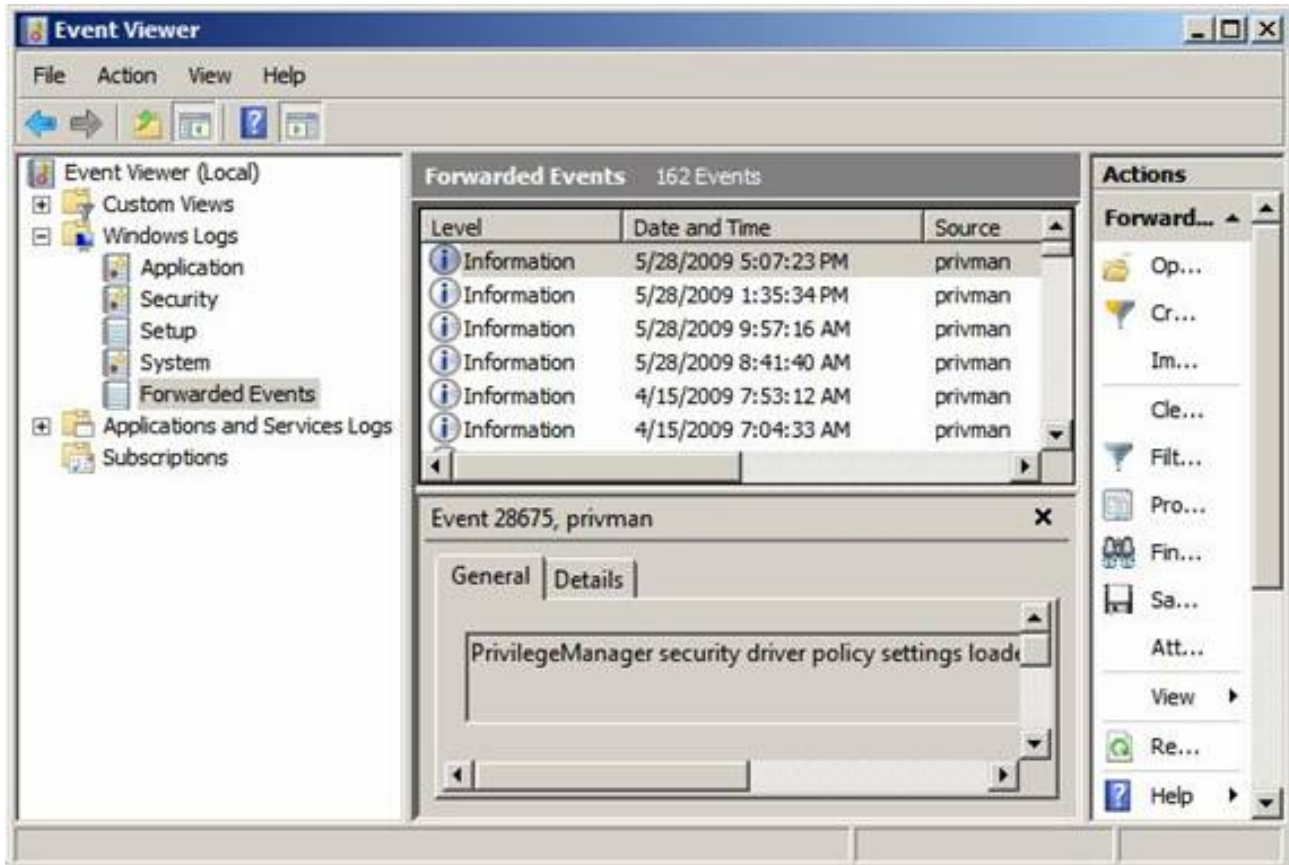


Figure 6: Events collected by Windows XP and sent to a Windows Server 2008 centralized log computer

Summary

Microsoft has come to the rescue if you are responsible for managing and reviewing event logs. There is new technology in Windows Server 2008 and Windows Vista that allows you to create a centralized logging computer. Once you have the centralized log computer set up, you only need to initialize the Remote Management component on your source computer. The source computer can be Windows XP SP2, Windows Server 2003 SP1, Windows Vista, or Windows Server 2008. Subscriptions are set up on the centralized log computer. All you do is to establish which computers you want to collect from, as well as which events you want to obtain. With regards to the other computers, you just review the centralized log computer's Event Viewer to see events from around the network whilst servicing them.